October 2025

CyberPeace

POLICY BRIEF

CYBERPEACE ANALYSIS AND COMMENTARY

Department- Related Parliamentary Standing Committee on Home Affairs

THE 254th REPORT ON CYBER CRIME - RAMIFICATIONS, PROTECTION AND PREVENTION

About CyberPeace

CyberPeace Foundation is a global non-profit think tank of experts and researchers working to promote cyber peace and trust in technology. Through multi-stakeholder engagement, policy advocacy, and capacity building, it strives to ensure a safe, secure, and equitable cyberspace for all.

Disclaimer

For more information

Visit www.cyberpeace.org

Author

Ayndri
Research Analyst,
Policy & Advocacy, CyberPeace

CONTENTS

ABBREVIATIONS

Abbreviation	Full Form
AI	Artificial Intelligence
API	Application Programming Interface
C-DAC	Centre for Development of Advanced Computing
CBoM	Cryptographic Bill of Materials
CBI	Central Bureau of Investigation
CERT-In	Indian Computer Emergency Response Team
DFS	Department of Financial Services
DoSEL	Department of School Education and Literacy
DoT	Department of Telecommunications
DSPE Act	Delhi Special Police Establishment Act
EU	European Union
FIR	First Information Report
I4C	Indian Cyber Crime Coordination Centre
IT	Information Technology
MeitY	Ministry of Electronics and Information Technology
MEA	Ministry of External Affairs
MNVS	Mobile Number Validation Services

ABBREVIATIONS

Abbreviation	Full Form
MHA	Ministry of Home Affairs
NCIIPC	National Critical Information Infrastructure Protection Centre
NCW	National Commission for Women
NCRB	National Crime Records Bureau
NCRP	National Cybercrime Reporting Portal
NIA	National Investigation Agency
NPCI	National Payments Corporation of India
OTT	Over-the-Top (media platforms)
PFRDA	Pension Fund Regulatory and Development Authority
QR	Quick Response (code)
RBI	Reserve Bank of India
RE	Regulated Entities
SEBI	Securities and Exchange Board of India
SIM	Subscriber Identity Module
SSMI	Significant Social Media Intermediary
UPI	Unified Payments Interface
TRAI	Telecom Regulatory Authority of India
UNODC	United Nations Office on Drugs and Crime

EXECUTIVE SUMMARY

India's growing digital adoption has exposed individuals, businesses, and national infrastructure to escalating cyber threats. These trends have caused financial losses and eroded public trust in digital systems. Against this background, the Department-Related Parliamentary Standing Committee on Home Affairs has released its 254th report on "*Cyber Crime - Ramifications, Protection and Prevention",* consolidating cybercrime trends, impacts, legal provisions, and recommendations to combat cyber threats.

Between 2019 and 2024, over ₹31,594 crore was defrauded across 53.93 lakh complaints, primarily through financial crimes. Rising threats include ransomware, DDoS attacks, AI-driven fraud, and deepfake-enabled scams. Vulnerable groups, including women, youth, and marginalised communities, face disproportionate harm.

Key gaps include underreporting, fragmented grievance mechanisms, slow LEA coordination, and a lack of sectoral cybersecurity capacity. The report recommends unified cyber laws, institutional capacity building, data governance reforms, and citizen-centric awareness programs to strengthen India's cyber resilience.

However, while the recommendations provide a robust foundation, some proposals risk undermining fundamental rights such as freedom of speech, privacy, and creative expression.

Dissenting perspectives emphasise that cybercrime measures must be precise, proportionate, and constitutionally sound. Alternatives like establishing an independent oversight tribunal, enabling cooperative inter-agency coordination, and incentivizing self-regulation in digital media platforms can ensure that security objectives are met without compromising democratic freedoms.

Ultimately, India's cyber policy must strike a judicious balance: fighting cybercrime effectively while safeguarding the rights and liberties that form the foundation of a healthy democracy.

Note: CyberPeace advocates for, and has used of the term "survivor" insteasd of "victim" in this brief to refer to those who have been victimised by cyber offenders. This is to shift focus from the aggrieved as a passive subject to an active beacon of hope and resilience.

INTRODUCTION

The Department-related Parliamentary Standing Committee on Home Affairs recently presented its 254th Report on "*Cyber Crime - Ramifications, Protection and Prevention*" in the Rajya Sabha and the Monsoon Session of the 18th Lok Sabha. While cybercrime has been a part of Parliamentary discourse, it has been spread across sector-specific reports and Parliament questions and answers. The 254th report is among the first to examine cybercrime in an overarching manner, consolidating the trends, impacts, protection mechanisms, and key legal provisions, and provides recommendations.

The Committee selected this subject in October 2024. It engaged with a wide spectrum of stakeholders, including the Ministry of Home Affairs and the Indian Cyber Crime Coordination Centre (I4C), the Ministry of Electronics and IT (MeitY), the Ministry of External Affairs (MEA), financial regulators such as RBI and SEBI, leading banks, telecom authorities (DoT and TRAI), investigative agencies like CBI and NIA, and technical bodies including CERT-In, NCIIPC, NIC, and C-DAC. Inputs were also sought from industry representatives, educational departments, and domain practitioners, including experts from CyberPeace. Drawing upon these consultations, written submissions, and background notes, the Committee finalised and adopted its 254th Report on 18 August 2025.[1]

BACKGROUND

India's growing digital adoption, driven by widespread internet access and mobile connectivity, has received global recognition. However, this also raises the issue of proliferating and rapidly evolving cybercrime.

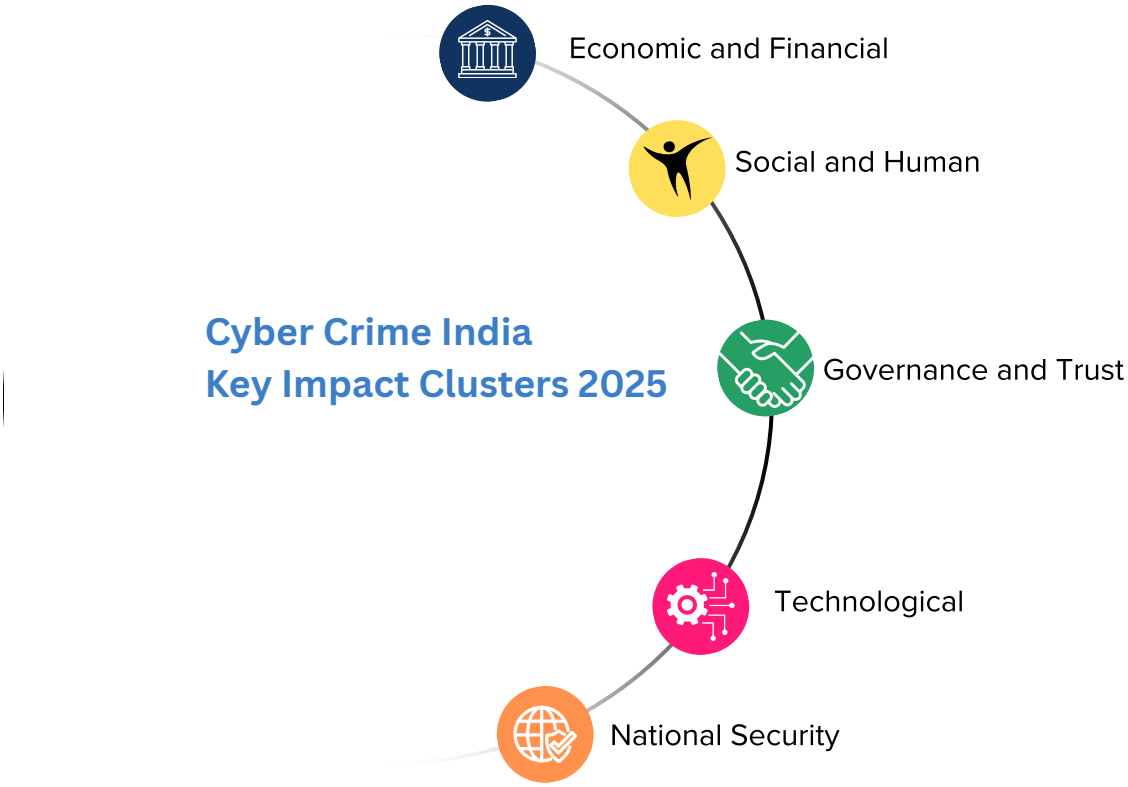
Individuals, companies, governments, and national critical infrastructure are increasingly susceptible to offences such as social engineering attacks, ransomware incidents, Distributed Denial of Service attacks (DDoS), and data breaches. Such attacks are growing in volume and velocity, giving rise to new modalities of crime[2] like cryptojacking, use of fileless malware, and increasingly elaborate social engineering attacks including digital arrest scams. Further, the use of AI has not only made attacks faster and easier to commit, but also given rise to new types of fraud, such as the use of deepfakes to clone voices and images. It also makes it easier for individuals without advanced technical skills to launch attacks and target at scale or outsource them through cybercrime-as-a-service (CaaS) providers. With rising geopolitical tensions, cyber tools are also being used increasingly to commit direct attacks on national infrastructure and conduct grey zone warfare through misinformation campaigns.[3][4]

Cybercrime presents an all-encompassing threat to the global social, economic and political order. The World Economic Forum has recognised cybercrime as one of the top ten global risks. It can cause financial losses, privacy violations, psychological trauma, breach of trust in organisations[5] and governments, disrupt services, break down social relationships, and jeopardise national security. This holistic report by the Department-related Parliamentary Standing Committee on Home Affairs is thus timely and vital for informing future direction for policymakers, industry, and civil society alike. A QR has been inserted in Annexure A for anyone who wishes to refer to the original report.

[1] Pg (ii), Two Hundred Fifty Fourth Report of the Department-Related Standing Committee on Home Affairs at https://www.medianama.com/2025/09/223-guide-parliamentary-panels-254th-report-cybercrime-india/
[2] Pg 1, ibid.
[3] Pg 4, ibid.
[4] Pg 5, ibid.
[5] Ibid.

KEY TRENDS

The report highlights trends across five key clusters:



Economic & Financial Trends

- Over ₹31,594 crore defrauded across 53.93 lakh complaints on the National Cybercrime Reporting Portal (NCRP) between 2019 and 2024: (NCRP).
- Of these, cyber financial crimes account for 85 % of the complaints: (NCRP)
- Ransomware is among the most “debilitating” forms of cybercrime for individuals and organisations, both: (MHA)
- DDoS attacks disrupting businesses, government services, and critical infrastructure: (MHA)
- Mule accounts are a big pain point in the financial sector: (RBI)
- Small banks and cooperative institutions are particularly vulnerable due to the lack of end-to-end transaction monitoring: (RBI)
- Response time gaps and escalation failures in many banks: (DFS)

- **UPI, QR code, and payment gateway frauds** are rising due to weak APIs, insecure third-party aggregators, and low customer awareness: (NPCI)

- **SIM swaps, closure frauds, spoofed calls** used for banking fraud, and OTP theft: TRAI

Social and Human Trends

- **AI and machine learning** are expected to shape the future of cyber threats to individuals and organisations, both: (MHA)

- Individuals are prone to **investment and trading scams**, including fraudulent stock market schemes, cryptocurrency frauds, digital arrest scams, **dating and romance** scams, and **fake job offer** scams: (MHA)

- Indian citizens are **trafficked** abroad and coerced to perform scams on others: (CBI)

- Survivors of **sextortion, identity theft, cyberstalking, and synthetic media-enabled fraud** may face severe mental health consequences (anxiety, depression, trauma) due to self-blame, stigma, and shaming.

- **Cyberbullying** among school children is on the rise, causing emotional distress, low self-esteem, and declining academic performance: (DoSEL)

- Organised international cybercrime units are recruiting **unemployed** men and women to conduct illegal activities such as managing mule accounts: (MHA, C-DAC)

- Overall impact: **mental health, increasing disempowerment, and social isolation**.

National Security Trends

- Agencies (MEA, CBI, DoT, I4C) recognize cybercrime syndicates, cyberterrorism, and hostile actors as direct threats to **national sovereignty and stability**.

- **Ransomware attacks on critical infrastructure** have national security implications: (MeitY, I4C, CERT-In)

- Malicious actors exploit **asymmetries** across national legal frameworks, regulatory systems and law enforcement capacities to conduct cross-border cybercrimes.

- **Traditional criminal enterprises and cyber-enabled crimes are convergin**g to conduct money laundering and trafficking operations: (UNODC)

- South East Asia is growing as a hub for **cybercrime-as-a-service,** with the sale of phishing kits, ransomware, deepfake tools, and laundering services.

- Employment fraud has been facilitating the **human trafficking** of unemployed youth.
- Slow extradition and real-time data sharing, along with a lack of standardised global frameworks, present **diplomatic and legal challenges**.

Technological Trends

- **Dark web** marketplaces and **encrypted apps** are used for narcotics, arms, fake IDs, and child exploitation.
- Encrypted messaging and **VPNs** facilitate extremist recruitment and illicit payments.
- **SIM cards** acquired in bulk through shell entities are shipped offshore to activate WhatsApp accounts used for impersonation-based fraud.
- **WhatsApp and Telegram** are utilised to solicit bank accounts for use as mule accounts.
- A **multimodal financial infrastructure** using peer-to-peer cryptocurrency transactions, purchase of physical assets (e.g., gold), offshore cash withdrawal points, and international fintech platforms is being used for laundering proceeds from fraud.
- AI-**driven fraud & deepfakes** are being used to mimic voices and faces in real time, to trick people into transferring funds. These attacks challenge traditional forensic detection.
- **Misconfigured cloud systems and poor encryption** affect the healthcare and education sectors.
- Most public/semi-public institutions **lack trained in-house cybersecurity staff**.
- **IoT devices, routers, and mobile network**s are susceptible to botnet attacks. As 5G expands, the number of attack vectors increases.
- Coding bootcamps and **unsupervised digital learning platforms** sometimes equip youth with advanced technical skills that may be diverted into malicious activities.

Governance and Trust Trends:

- **Trust deficit** in digital platforms & UPI due to rising frauds (phishing, QR scams, OTP bypass, deepfakes) visible through elderly users and small merchants reverting to cash, reversing gains of Digital India.
- **Harms are gendered since women face disproportionate** privacy anxiety, harassment, and trauma from deepfake-based abuse.

- Universities and research institutes face ransomware/data breaches, leading to **hesitancy toward online learning**.
- **Schoolchildren are exposed** to inaccurate educational content and inappropriate material.
- **Weak user protection by financial institutions** was noted. Unauthorised debits failed to be blocked, and customer support often **delays reversal/refund**, compounding distrust.
- Helplines (1930), NCRP portal, and grievance redressal mechanisms exist but are **slow, under-resourced, and fragmented**.
- NCRP recorded **53.93 lakh complaints till Nov 2024**, but FIR conversion is significantly lower.
- **Financial fraud dominates complaints** (via CFCFRMS).

POLICY IMPLICATIONS OF TREND ASSESSMENT

The 254th Report highlights several important cybercrime trends. Since the committee's recommendations are based on the inferences drawn from these, it is essential to examine them closely. **Additionally, any assessment gaps offer guidance for further research in order to fully comprehend the economic and social effects of cybercrime in India.**

Theme	Key Gaps Identified	Implications
Data & Measurement	• NCRP's 53.93 lakh complaints reflect only *reported* cases, and not the large volume of unreported or unregistered incidents due to stigma, lack of awareness about reporting mechanisms, or low trust in grievance redressal. • No clear link between reported cases and long-term macroeconomic risks. • No sectoral breakdown (banking, retail, health, telecom) of ₹31,594 crore in reported losses.	• If policymakers rely only on reported numbers, resource allocation (budgets, manpower, institutional support) will be under-calibrated compared to the actual need. • Cybercrime is not just a law-and-order issue. Valuation of indirect costs, productivity losses, investment climate risks, target profiles and financial stability risks is required to formulate a long-term strategy. It also requires interdisciplinary expertise from fields such as criminology and sociology in order to design accurate policies for crime prevention and organisational resilience. • Lack of a sectoral breakdown obscures which industries are most exposed, formulation of targeted interventions, and hampers international benchmarking of India's cyber resilience

Theme	Key Gaps Identified	Implications
	• No comparative benchmarking of figures with global economies (e.g., proportion of GDP lost, fraud typologies, trust erosion).	• Hampers understanding of scale and impact, and deprives policymakers of insights from economies that have successfully addressed similar fraud typologies.
Survivors & Society	• No disaggregated profiling by gender, caste, age, or geography, despite evidence that women, LGBTQ+ persons, and marginalised groups are disproportionately affected. • Insufficient granular evidence or data on cybercrime experiences of rural youth, students with disabilities, and female students. • The hidden psychological toll (fear, stigma, mental health impacts) remains unquantified. • Long-term social impacts on career loss, family strain, and mistrust in the digital economy are not assessed.	• Cybercrime policies may not adequately protect the very groups who are most at risk, resulting in blind spots in prevention, survivor support, and trust in digital systems. • As above. • Weakens support for mental health services, survivor protection frameworks, and risks leaving survivors isolated or unwilling to report incidents, thereby perpetuating underreporting. • As above.

KEY RECOMMENDATIONS OF THE REPORT

The report highlights recommendations across four key clusters:

Legal & Regulatory Reforms

- Unified Cybercrime Law with Integrated Cybercrime Task Force.[6]
- Review intermediary safe harbour protections[7] and assign accountability for failure to comply with lawful takedown orders within prescribed timelines.[8]
- OTT content monitoring pre- and post-release.[9]
- App compliance with data protection laws[10]; regulate offshore advertisers.[11]
- Regulate telecommunication channels; invest in indigenous tech (ASTR).[12]
- Recipient approval for incoming money to reduce mule accounts.[13]
- SEBI oversight of financial influencers on social media.[14]
- Oversight of online gaming platforms.[15]
- VPN logging with judicial oversight.[16]
- Strengthen MLATs[17] and establish the International Cybercrime Liaison Unit.[18]
- Mandatory IT intermediary registration and local grievance officers.[19]
- Amend IT Act: harsher punishments, reduced bailability, intermediary liability.[20]
- Assign cybercrime cases to trained senior officers.[21]
- Periodic legislative review of cybercrime laws.[22]

Institutional Capacity and Enforcement Reforms

- Enhance inter-agency coordination (TRAI, RBI, MeitY, DFS, SEBI, NPCI, CERT-In, etc.).
- Cyber-threat expert vertical in TRAI to address quantum threats.[23]
- Expand RBI's CFCFRMS to smaller banks[24]; strengthen Ombudsman capacity.[25]
- Regulated Entities (RE) to develop a Cryptographic Bill of Materials (CBoM)for quantum-safe tech.[26]
- SEBI: multi-layered cybersecurity, audits, risk monitoring.[27]

[6] 4.1.18, ibid.
[7] 3.2.15, ibid.
[8] 3.2.16
[9] 3.2.17
[10] 3.2.19
[11] 3.3.4, ibid.
[12] 3.4.10
[13] 3.6.38
[14] 3.8.9
[15] 4.1.7
[16] 4.1.7
[17] 3.13.5, ibid.
[18] 4.1.9, ibid.
[19] 4.1.8
[20] 4.1.10
[21] 4.1.12
[22] 4.1.13
[23] 3.5.17
[24] 3.6.33
[25] 3.6.36
[26] 3.6.37
[27] 3.8.8

- Curb unregistered financial influencers[28] through AI monitoring and awareness campaigns[29].
- Expand NPCI real-time fraud monitoring[30].
- Amend DSPE Act for nationwide CBI cybercrime jurisdiction[31].
- Early data preservation protocols; timely SSMI access to NIA[32].
- State Cybercrime Coordination Centres (S4C) in all States/UTs[33].
- CERT-In: AI-driven threat intelligence; cross-sector drills; academia partnerships[34].
- Sector-specific CSIRTs with a central coordination hub[35].
- Immediate suspension of suspicious financial transactions[36].
- Cybersecurity course for police recruitment[37].
- LEA capacity building: training, research centers, advanced forensic labs[38].

Technology & Data Governance

- Watermarking/media provenance frameworks for AI content[39].
- Age verification and parental controls on OTT platforms[40].
- Integrate grievance redressal with data protection frameworks[41].
- Indigenous app store for startups[42].
- Automate data flow between Sanchar Saathi, Digital Intelligence Platform, LEAs[43].
- Nationwide Mobile Number Validation Services (MNVS)[44].
- Central blacklist of Unregistered Telemarketers (UTMs)[45].
- Expand MuleHunter.ai; strengthen anti-mule account measures[46].
- Standardize financial platforms: UI/UX, interoperable APIs, data portability[47].
- C-DAC: AI/ML predictive threat intelligence; VR-based cybersecurity training[48].

[28] 3.8.10
[29] 3.8.10
[30] 3.9.8
[31] 3.10.15
[32] 3.10.30
[33] 3.11.10
[34] 3.15.6
[35] 3.12.9
[36] 4.1.14
[37] 4.1.15
[38] 4.1.16
[39] 3.2.13
[40] 3.2.17
[41] 3.2.14
[41] 3.2.19
[43] 3.4.8, ibid.
[44] 3.4.8, ibid.
[45] 3.5.18
[46] 3.6.35
[47] 3.7.4
[48] 3.14.8

Citizen-Centric Capacity Building and Public Awareness

- Standardize complaint filing; clear timelines; public grievance statistics[49].
- Multi-lingual awareness campaigns, especially regional/rural[50].
- Train bank staff and customers on fraud methods [51].
- RBI: educate customers about genuine ".bank.in" domains[52].
- Personalize liability limits; incentivize strong digital hygiene[53].
- Consumer protection: micro-insurance, AI liability reduction, zero-liability periods, support for vulnerable groups[54].
- Cyber literacy in school curricula; mandatory cyber education in higher education[55], [56].
- Community networks to detect and report mule accounts[57].

POLICY IMPLICATIONS OF RECOMMENDATIONS

Report Recommendation	Policy Implications / Gaps
VPN logging mandates (Rec 4.1.7)	• While the recommendations account for safeguards for data retention and reporting obligations, their scope requires clarification. • CERT-In's 2022 direction under the IT Act mandating data retention for VPN service providers is in contention with the storage limitation and erasure rights granted by the DPDP Act. • Log retention risks being unconstitutional on grounds of being violative of user privacy, economically counterproductive (some VPNs have exited India), and being harmful to user trust.
Actions recommended for I4C (Rec. 3.11)	• I4C currently functions under an executive order and may lack the powers to effectively tackle cybercrime[58].
CBI cybercrime powers (Rec. 3.10)	• Amending the Delhi Special Police Establishment (DSPE) Act to allow CBI investigations without state consent will undermine cooperative federalism[59], which is central to India's constitutional design.

[49] 3.2.14,
[50] 3.4.9
[51] 3.6.31
[52] 3.6.32
[53] 3.6.40
[54] 3.6.41
[55] 3.6.42
[56] 3.16.7
[57] 3.7.5
[58] Sh. Haris Beeran, Dissent Note and Proposed Amendments to the Recommendations in the Draft Two Hundred Fifty-Fourth Report on 'Cyber Crime - Ramifications, Protection and Prevention, Department-Related Parliamentary Standing Committee on Home Affairs, Rajya Sabha, pg no.115-116, 2025.
[59] Ibid.

Report Recommendation	Policy Implications / Gaps
Safe harbour review (Recs. 3.2.15 & 4.1.7)	• Vague review could dilute intermediary immunity, risking over-censorship and licensing-by-stealth[60].
Penalties & platform suspension for social media intermediaries (Rec. 3.2.16)	• The executive power to suspend platforms is disproportionate and may be used punitively; it may suppress dissent and harm independent media.
Mandatory OTT pre-certification (Rec. 3.2.17)	• Centralised pre-certification is operationally impractical due to diversity in content. It jeopardises artistic freedom and creativity, affects employment, and may censor news/documentaries[61].
Mandatory IT intermediary registration (Rec. 4.1.8)	• A registration-based model may have a chilling effect on startups experimenting with innovative offerings, facing the risk of arbitrary market denial[62]. • Lack of clarity in the scope of "all" intermediaries risks overregulation of small players and vagueness regarding foreign startups operating in India. • Data security, breach notification, or misuse prevention for the registry is a task in itself.
Court orders vs government alerts (Paras 3.2.16 & 4.1.11)	• Vague "government alerts" could force over-compliance, suppress speech.
Cybercrime Definitions	• Current definition lumps crimes committed by minors, less serious, and organised crimes together[63].
Survivor Support	• The report has minimal recommendations on survivor support. Instead of treating survivors (individuals, groups and organisations) as incidental beneficiaries of institutional and enforcement reforms, it is important to recognise that these are the central stakeholders affected by the digital economy of crime. • Strategies for offender prevention need ot be explored. For this, a multidisciplinary approach will be required. • Special vulnerabilities like online child exploitation, cyberstalking, gendered harms, or digital illiteracy among the elderly are relatively unaddressed.

[60] Sh. Ajay Makan, *Final Dissent Note on the 254th Draft Report on 'Cyber Crime – Ramifications, Protection and Prevention'*, Department-Related Parliamentary Standing Committee on Home Affairs, Rajya Sabha, pg no. 118- 123, 2025.
[61] Ibid.
[62] Ibid.
[63] Smt Priyank Gandhi Vadra, Proposed Amendments to the Recommendations in the Two Hundred and Fifty Fourth Draft Report on 'Cyber Crime – Ramifications, Protection and Prevention', Department-Related Parliamentary Standing Committee on Home Affairs, Rajya Sabha,pg no.124-129, 2025.

CYBERPEACE ANALYSIS AND COMMENTARY

The 254th Parliamentary Standing Committee Report is hailed by the CyberPeace Foundation as a vital step in comprehending and tackling India's changing cyber threat environment. Notably, the Committee provides policymakers, regulators, and civil society with a useful framework, thanks to its comprehensive approach, which encompasses the economic, social, technological, and governance aspects. Focusing on new threats like ransomware, deepfakes, AI-driven fraud, and cybercrime-as-a-service is in line with worldwide patterns. It emphasises how urgent it is to take preventative action.

However, some suggestions raise issues with innovation, privacy, and proportionality. Broad restrictions on OTT pre-certification, VPN logging, and intermediary registration run the risk of jeopardising user confidence, free speech, and innovation. CyberPeace emphasises the significance of incorporating independent oversight and constitutional protections in this regard.

More survivor-centric reforms are also required, considering the reality of intersectional harms and their psychosocial impact on individuals in society. To guarantee inclusion and protection for vulnerable groups, CyberPeace advocates for community-based reporting systems, disaggregated data collection, and comprehensive survivor assistance frameworks.

In summary, CyberPeace stresses a balanced strategy that incorporates technological innovation and rights-respecting governance, even as the report establishes a solid foundation for cybercrime prevention and enforcement. India can create a safe, robust, and just cyber ecosystem by implementing the Committee's recommendations in conjunction with constitutional protections, focused survivor assistance, and cross-sector cooperation.

WAY FORWARD

Legal and Regulatory Reforms

India’s cybercrime governance framework needs legislative reform that strengthens accountability without enabling overreach or having a chilling effect on innovation.

- **Differentiated Cybercrime Classification Framework:** Differentiate crimes by severity (minor vs serious), age of perpetrator (minors), and nature (privacy violations, organized attacks by corporations/political entities[64]

- **Balanced VPN Regulation:** Any VPN data retention or logging obligations must align with the principles of *purpose limitation* and *proportionality* under the DPDP Act, 2023. Retention should be targeted, triggered only through specific investigations authorised by judicial orders, and subject to independent audits. Blanket retention mandates risk breaching privacy guarantees and deterring legitimate service providers.

[64] Ibid.

- **Safe Harbour Accountability:** Intermediary liability must be linked only to *formal court or Section 69A orders* to prevent arbitrary enforcement. However, since Section 69A itself is opaque, any takedown or blocking orders must be publicly disclosed (with narrow redactions) and open to independent appeal or review. Government-mandated takedowns for harmful content cannot be the primary form of moderation. Intermediary accountability needs to be explored through incentivised content moderation practices and well-defined co-regulatory responsibilities. The law should also consider distinguishing between illegal content and harmful-but-legal content along the lines of the EU Digital Services Act, 2022.

- **Intermediary Accountability Enforcement:** Instead of suspending operations, proportionate monetary penalties can be imposed for non-compliance with reasoned court orders. The platform should also have the right to appeal the penalty before an independent judicial tribunal.[65]

- **Independent Digital Tribunal:** To check executive discretion, a Digital Tribunal can be established, headed by a retired High Court or Supreme Court judge, to review takedown orders, platform penalties, and data-access requests. This ensures transparency, due process, and consistency in enforcement.[66]

- **Transparency in Intermediary Oversight:** Instead of a permission-based registry, which could lead to the risk of market denial for small businesses. Intermediaries may instead be required to publicly disclose their grievance/ nodal officers for 24x7 coordination with law enforcement [67]. A searchable database of Significant Social Media Intermediaries (SSMIs) can be maintained to enhance public accountability without creating entry barriers for smaller startups.

Institutional and Enforcement Reforms

The current institutional framework for cybercrime response relies heavily on executive orders and fragmented coordination. Structural strengthening and statutory clarity are essential to improve enforcement.

- **Centre-State Enforcement Coordination without Overreach:** Amending the DSPE Act to allow the CBI to bypass state consent could undermine cooperative federalism. To avoid this and address the challenges presented by ad hoc coordination, a legal framework for inter-LEA coordination should be established, which codifies protocols for joint investigations, shared jurisdiction, data access, and real-time coordination mechanisms between central agencies like CBI, NIA, I4C, and state LEAs, along with their cybercrime units.

- **Early Data Preservation and Forensics:** Standardised data preservation protocols should mandate state police to initiate preservation requests within 24 hours of a cybercrime report. This must be balanced with privacy safeguards and audit trails under the DPDP framework.

- **Harmonised Institutional Ecosystem:** Coordination among regulators (RBI, SEBI, TRAI, CERT-In, DFS, DoT, MeitY, and NCIIPC) must be enhanced through interoperable reporting standards and unified cyber incident response mechanisms.

[65] Sh. Ajay Makan, *Final Dissent Note on the 254th Draft Report on 'Cyber Crime – Ramifications, Protection and Prevention'*, Department-Related Parliamentary Standing Committee on Home Affairs, Rajya Sabha, pg no. 118- 123, 2025market-denial.
[66] ibid.
[67] Ibid.

Technology and Data Governance

Cyber governance must move beyond compliance checklists to privacy-preserving, interoperable, and innovation-supportive data systems.

- **Targeted Logging and Data Governance:** Any form of data collection or retention should comply with DPDP principles, specifically *purpose limitation*, *storage limitation*, and *security safeguards*. Blanket logging or data retention should be replaced with *selective, court-sanctioned access* backed by audit trails.

- **Interoperable and Secure Financial Systems:** Regulators (RBI, SEBI, IRDAI, PFRDA) should adopt standardised UI/UX guidelines, interoperable APIs, and data portability frameworks to ensure consumer security and transparency across financial platforms.

- **Transparency and Risk Communication:** Periodic public disclosure of breach notifications, intermediary compliance audits, and cybercrime trends should be institutionalised to build citizen trust and accountability.

- **OTT Governance:** Instead of pre-certification, which often has the same effect as censorship, all platforms can be mandated to self-classify content, and a co-regulatory model for OTT platforms can be explored. Provisions mah be set up for fast post-publication grievance redressal[68]. There is also a need for setting guardrails for robust age-assurance and increased public awareness on parental controls aligned with data protection principles and international best practices (e.g., EU Audiovisual Media Services Directive).

Survivor-Centric Reforms

Survivors remain the least represented group in India's cybercrime policy. Future reforms must adopt a survivor-first approach, integrating psychological, social, and procedural support.

- **National Survivor Assistance Framework:** Establish a Cybercrime Survivor Assistance Scheme providing legal aid, trauma counselling, and quick compensation. This could operate as a joint initiative between MHA, NCW, and MeitY.

- **Disaggregated Survivor Data:** Mandate the collection and publication of disaggregated survivor data (by gender, caste, class, sexuality, disability, and location) to inform targeted interventions and funding priorities.

- **Protection of Vulnerable Groups:** Introduce tailored survivor-protection protocols for children, elderly citizens, and LGBTQ+ persons, ensuring child-friendly reporting systems, priority case handling, and anonymity for survivors of cyber sexual harassment or doxxing.

[68] Ibid.

- **Community-Based Reporting and Awareness:** Expand public awareness programs into an assisted reporting infrastructure through Panchayats, self-help groups, NGOs, and local cyber desks. Offline reporting kiosks linked to the NCRP portal can be deployed in rural areas.

- **Rehabilitation for Trafficking Survivors:** Establish cross-border repatriation protocols and rehabilitation programs for survivors of cyber-enabled human trafficking and labour exploitation, integrating efforts by MEA, MHA, and NCW.

CONCLUSION

India stands at a critical juncture in its digital transformation journey, facing a rapidly intensifying cyber threat environment. The 254th Parliamentary Standing Committee Report offers an unprecedented, holistic diagnosis of cybercrime's multifaceted impacts and lays a strong foundation for reform.

Balancing robust cybercrime deterrence with the protection of democratic freedoms is paramount. By embracing cohesive laws, institutional strengthening, innovative technologies, and inclusive citizen empowerment, India can build a cyber ecosystem that is secure, trusted, and resilient.

Sustained political will, cross-sector collaboration, and vigilant protection of fundamental rights will be indispensable in realizing this vision. With thoughtful implementation and continued adaptive governance, India can safeguard its digital future while fostering innovation and inclusion in the cyber age.

Annexure A: QR OF OFFICIAL REPORT

https://www.medianama.com/wp-content/uploads/2025/08/rsnew_Committee_site_Committee_File_ReportFile_15_197_254_2025_8_12-1.pdf

About CyberPeace

CyberPeace is a global non-profit organization headquartered in India, working at the intersection of cybersecurity, policy, and peacebuilding. It envisions a safe, resilient, and inclusive cyberspace for all.
Through its global initiatives, CyberPeace drives capacity building, policy research, incident response, and public awareness to advance the vision of "CyberPeace and Trust in Technology." From grassroots digital literacy programs to high-level policy and research collaborations, CyberPeace integrates innovation, education, and advocacy to strengthen digital ecosystems worldwide.
Championing the future of responsible technology, CyberPeace is building the next generation of Cyber Defenders and Responsible Digital Citizens, aligning its mission with the United Nations Sustainable Development Goals (SDGs) and India's Viksit Bharat 2047 vision.


CyberPeace